Title	2個の生成元を持つFree IN-Algebra及びFree ICN-Algebraの決定 (数理論理とモデル理論)
Author(s)	佐藤, 雅彦
Citation	数理解析研究所講究録 (1973), 180: 10-19
Issue Date	1973-06
URL	http://hdl.handle.net/2433/107136
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

数理解析研究所講究録
180巻 1973年 10-19

2個の生成元を持つ free IN-algebra 及び free ICN-algebra の決定

東大 理　佐藤雅彦

よく知られているように，直観主義命題論理は決定可能であり，任意に論理式を与えたときにそれがLJの定理であるかどうかを決定する program もいくつか存在している（例えば 吉森［4］，嶋田［7］）。また Diego［2］，Mckay［5］によれば，有限個の命題変数を固定するとき，それらで生成される ICN-formula（∨を含まない formula）全体から作られる Lindenbaum algebra は有限であることが分っている。従ってこの Lindenbaum algebra の構造は，上の program を使えば原理的には決定可能である。しかしこのことは，計算時間の関係から現実的には，ほとんど不可能である。以下では，代数的な手法によって，この Lindenbaum algebra の構造を簡単に決定する一方法を与え，計算機による計算結果を簡単に述べる。

Def. 1 (I-algebra) $A=(A, 1, \to)$ は以下の条件を満たすとき I-algebra であるという。ただし $1 \in A$ で、$\to$ は A の上の binary operation である。

(I 1) $p \to (q \to p) = 1$

(I 2) $(p \to (q \to r)) \to ((p \to q) \to (p \to r)) = 1$

(I 3) $p \to q = q \to p = 1 \Rightarrow p = q$

Def. 2 $F \subset A$ は次の条件を満たすとき、A の filter であるという。

(F 1) $1 \in F$

(F 2) $p \in F,\ p \to q \in F \Rightarrow q \in F$

F による A 上の relation $\sim_F$ を、$p \sim_F q \Leftrightarrow p \to q \in F$, $q \to p \in F$ によって定めれば、$\sim_F$ は $\to$ と compatible な equivalence relation となるので、自然な方法で $A/\sim_F = A/F$ は I-algebra となる。また、$p \leqq q \Leftrightarrow p \to q = 1$ と定めれば、$\leqq$ は A 上に partial order を定める。1 はこの order での最大元である。

Diego [2] は有限生成の free I-algebra は有限であることを証明し、その構造を決定する constructive な方法を与えた。以下に定義する IN-algebra 及び ICN-algebra につい

ても Diego の証明はそのまま成立し，有限生成の free IN (ICN)-alg. は有限であることが分る。しかし，たとえば2個の生成元を持つ free IN(ICN)-alg. を Diego の方法で計算すると，相当な長時間計算になることが予測される。そこで，以下では IN(ICN)-alg. に特有なある性質を利用して，より効果的な方法を与える。東大数学教室の計算機 Tosbac 3300 を使って，この方法での計算時間は約10時間であった。

<u>Def. 3</u>　(IN-algebra)　$A=(A,1,\to,\neg)$ は次の条件を満たすとき IN-algebra であるという。ただし $\neg$ は A 上の unary operation である。

(I 1), (I 2), (I 3)

(N 1)　$(p\to\neg q)\to(q\to\neg p)=1$

(N 2)　$\neg p\to(p\to q)=1$

<u>Th. 4</u>　(Horn [3])

A が IN-algebra $\Longleftrightarrow$ A は最小元 0 を持った I-algebra で $\neg p$ は $p\to 0$ で定義される。

<u>Def. 5</u>　(ICN-algebra)　$A=(A,1,\to,\neg,\wedge)$ は次の条件を満たすとき ICN-alg. であるという。ただし $\wedge$ は

A 上の binary operation である。

(I1), (I2), (I3)

(N1), (N2)

(C1) $(p \wedge q) \rightarrow p = 1$

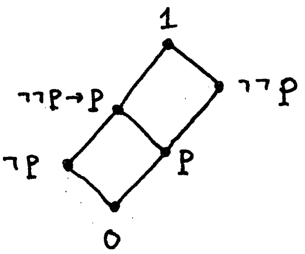
(C2) $(p \wedge q) \rightarrow q = 1$

(C3) $(p \rightarrow q) \rightarrow ((p \rightarrow r) \rightarrow (p \rightarrow (q \wedge r))) = 1$

<u>Th. 6</u> (Horn [3])

A が ICN-alg. $\Longleftrightarrow$ A は IN-alg. で $p \wedge q$ は $\inf\{p, q\}$ で定義される。

n 個の文字 $P_1, P_2, \cdots, P_n$ で生成される free ICN-alg. を $\lambda_{ICN}(n)$ (あるいは単に $\lambda(n)$) と書くことにする。Nishimura model [6] を見れば、$\lambda_{ICN}(1)$ は簡単に分り次のようになる。



この場合 $\lambda_{ICN}(1) = \lambda_{IN}(1)$ である。また $\lambda_I(1) =$ 

である。

$\lambda(m)$ は Diego の方法で finite であることが分るが，このとき McKay [5] によれば $\lambda(m)$ は，その順序 $\leqq$ によって，distributive lattice になる。一方 finite distributive lattice については次の表現定理（Th. 7）がある（Birkhoff [1] 参照）。

partially ordered set K に対して $\mathcal{O}_K \subset \mathcal{P}(K)$ を次のように定めれば，$\mathcal{O}_K$ は K 上の topology を定める。

$$L \subset K \text{ のとき } L \in \mathcal{O}_K \Longleftrightarrow (p \in L,\ q \leqq p \Rightarrow q \in L)$$

$\mathcal{O}_K$ の元の含包関係 $\subset$ を順序 $\leqq$ と思えば，よく知られているように $\mathcal{O}_K$ は pseudo-Boolean algebra になり，従って distributive lattice になる。また，lattice P の元 a は $a = p \vee q \Rightarrow a = p$ or $a = q$ となるとき join irreducible であるという。

Th. 7　P を finite distributive lattice とし，0 以外の P の join irreducible な元全体を K とすれば

$$P \cong \mathcal{O}_K$$

Def. 8　I-algebra P において，P − {1} が最大元（2 と書く）を持つとき P は irreducible であるという。

Th. 9　P を finite distributive lattice とし，$p \in P$ で生

成される filter を (p) とすれば,

$$p \text{ は } 0 \text{ でなく join irreducible}$$
$$\Longleftrightarrow \quad P/(p) \text{ は irreducible}$$

以下, $P = \lambda_{ICN}(m)$ $(m \geqq 1)$ を fix して考える。P を決定するには, Th. 7 によれば P の nonzero join irreducible element 全体 K を決定すればよい。$p \in K$ のとき, Th. 9 によれば, $Q_p = P/(p)$ は irreducible である。$R_p = Q_p/\{1,2\}$ とおく。このとき, 次のことが成立する。

Th. 10 $\quad \exists \{g_1, \cdots, g_{m-1}\} \subset R_p$ s.t. $R_p = \overline{\{g_1, \cdots, g_{m-1}\}}$。ただし, $G \subset R_p$ のとき $\overline{G}$ は G で生成される R_p の ICN-subalgebra。

(証明) $R_p = \{1\}$ ならば $R_p = \overline{\phi}$ 故明らか。$\overline{\overline{R_p}} \geqq 2$ のときは, $\overline{\overline{Q_p}} \geqq 3$ である。故に $2_{Q_p} \neq 0, 1$。P の free generator を $p_1, \cdots, p_m$ とし, $\varphi_p : P \to Q_p$ は natural map とする。このとき $Q_p = \overline{\{\varphi_p(p_1), \cdots, \varphi_p(p_m)\}}$。また, $Q_p - \{2\}$ は Q_p の ICN-subalgebra であるから, ある i に対して, $2 = \varphi(p_i)$ となる。故に $Q_p - \{2\} \subseteq \overline{\{\varphi_p(p_1), \cdots, \varphi_p(p_{i-1}), \varphi_p(p_{i+1}), \cdots, \varphi_p(p_m)\}}$。$Q_p - \{2\} \cong R_p$ であるから証明は終った。

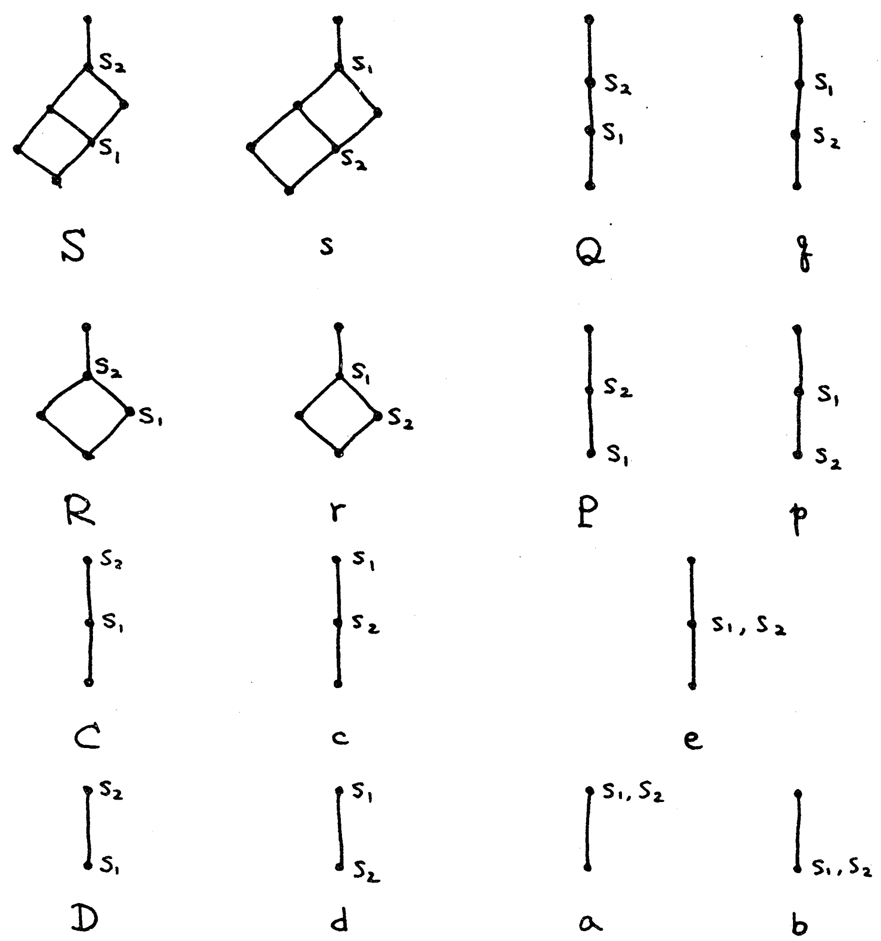
さて，Kの構造を決定するために，$p \in K$ に対して，$\mathbb{Q}_p = \langle Q_p ; \varphi_p(p_1), \cdots, \varphi_p(p_m) \rangle$ なる組を考える。また S を任意の irreducible ICN-alg. とし，$\{s_1, \cdots, s_m\} \subset S$ が $\overline{\{s_1, \cdots, s_m\}} = S$ を満たすとして，$\mathbb{S} = \langle S ; s_1, \cdots, s_m \rangle$ なる組全体の class $\mathcal{S}$ を考え，$\mathcal{S}$ 上の pseudo-order $\leqq^*$ を次のように定める。

$$\mathbb{S} = \langle S ; s_1, \cdots, s_m \rangle \leqq^* \mathbb{T} = \langle T ; t_1, \cdots, t_m \rangle$$

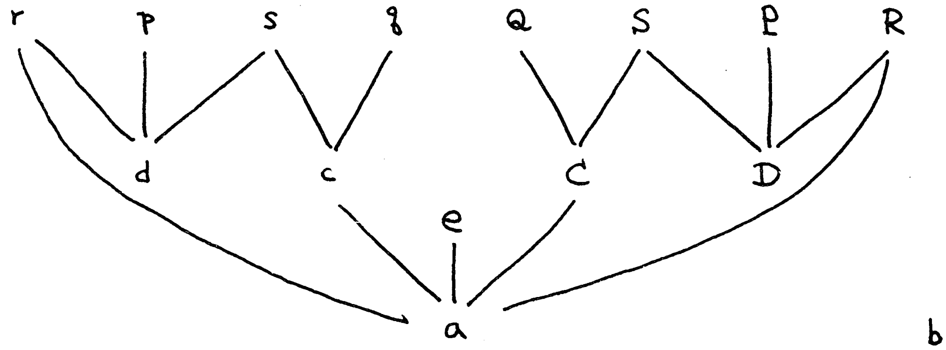
$\Longleftrightarrow$ $f(t_i) = s_i$ なる homomorphism $f : T \to S$ が存在する。

$p, q \in K$ とすれば，あきらかに，$p \leqq q \Longleftrightarrow (p) \supset (q)$ である。$\mathrm{Ker}\,\varphi_p = (p)$ 等に注意すれば，更に，$p \leqq q \Longleftrightarrow \mathbb{Q}_p \leqq^* \mathbb{Q}_q$ であることがわかる。$\leqq^*$ によって induce される equivalence relation を $\equiv$ とすれば，$\mathcal{S}/\equiv$ は ordered structure となり，P が free であるから各同値類の代表として $\mathbb{Q}_p$ の形をしたものを unique にとることができる。故に $\mathcal{S}/\equiv \,\cong K$ となる。また，Th. 10 の証明から，$Q_p/\{1,2\}$ は $\lambda(m-1)$ の homomorphic image となることがわかる。故に $\lambda(m-1)$ が知られていれば，$\mathbb{Q}_p$ の形はすべて決定できる。

以上の議論を $\lambda(2)$ について適用すれば，$\mathcal{S}/\equiv$ の代表は次の15組であることがわかる。但し，各図の下には K の元の名前が書かれてあり，$p \in K$ に対し，$\varphi_p(p_1) = s_1$，$\varphi_p(p_2) = s_2$ としてある。



またKのorderは次のようになる。



$\lambda(2)$ の generator を p_1, p_2 とすれば、上のことから

$$p_1 = c \vee d \vee a$$
$$p_2 = C \vee D \vee a$$

となる。 $\lambda(2) = \overline{\{p_1, p_2\}}^{ICN}$ であるが、 $\lambda(2) = \overline{\left(\overline{\{p_1, p_2, 0\}}^{I}\right)}^{C}$
また $\overline{\{p_1, p_2, 0\}}^{I} \cong \lambda_{IN}(2)$ であることが容易に分るので、
計算機では、まず $\overline{\{p_1, p_2, 0\}}^{I}$ を計算し、次に conjunction についての closure を計算した。

$\lambda_{IN}(2)$ は 518 個、$\lambda_{ICN}(2)$ は 2134 個あることが分った。
$\lambda_{IN}(2)$ の元で、LK の定理となるものは 126 個であった。
次頁に、$\lambda_{IN}(2)$ の元の最初の 20 個と最後の 18 個を示す。

References

[1] G. Birkhoff: Lattice theory, A.M.S. Colloq. Publ., vol. 25, 1948

[2] A. Diego: Sur les algèbres de Hilbert, Collection de Logique Mathématique, Série A, no. 21, Paris, 1966

[3] A. Horn: The separation theorem of intuitionistic propositional logics, J.S.L., 27 (1962), 391-399

[4] Y. Komori: Logics and their models (Japanese), Master thesis, Univ. Tokyo, 1972

[5] C. G. McKay: The decidability of certain intermediate propositional logics, J.S.L., 33 (1968), 258-264

[6] I. Nishimura: On formulas of one variable in intuitionistic propositional calculus, J.S.L., 25 (1960), 327-331

[7] K. Shimada: Master thesis, Tsuda College, 1973

$P \supset P$
$\sim(P \supset P)$
P
Q
$\sim P$
$\sim Q$
$Q \supset P$
$P \supset Q$
$\sim\sim P$
$\sim P \supset Q$

$Q \supset \sim P$
$\sim\sim Q$
$\sim Q \supset P$
$\sim Q \supset \sim P$
$\sim P \supset \sim Q$
$\sim(Q \supset P)$
$(Q \supset P) \supset P$
$(Q \supset P) \supset Q$
$\sim(P \supset Q)$
$(P \supset Q) \supset P$

$(((\sim\sim Q \supset Q) \supset P) \supset ((\sim\sim Q \supset P) \supset P)) \supset ((\sim\sim P \supset (\sim Q \supset P)) \supset ((\sim P \supset \sim Q) \supset P))$
$(((\sim\sim Q \supset Q) \supset P) \supset ((\sim\sim Q \supset P) \supset P)) \supset ((\sim\sim P \supset ((P \supset Q) \supset P)) \supset P)$
$(((\sim\sim Q \supset Q) \supset P) \supset ((\sim\sim Q \supset P) \supset P)) \supset ((\sim\sim P \supset ((P \supset Q) \supset P)) \supset ((Q \supset P) \supset P))$
$(((\sim\sim Q \supset Q) \supset P) \supset ((\sim\sim Q \supset P) \supset P)) \supset ((\sim\sim P \supset ((P \supset Q) \supset P)) \supset ((\sim P \supset Q) \supset P))$
$(((\sim\sim Q \supset Q) \supset P) \supset ((\sim\sim Q \supset P) \supset P)) \supset ((\sim\sim P \supset ((P \supset Q) \supset P)) \supset ((\sim Q \supset P) \supset P))$
$(((\sim\sim Q \supset Q) \supset P) \supset ((\sim\sim Q \supset P) \supset P)) \supset (((Q \supset \sim P) \supset P) \supset (((P \supset Q) \supset Q) \supset P))$
$(((\sim\sim Q \supset Q) \supset P) \supset ((\sim\sim Q \supset P) \supset P)) \supset ((\sim\sim P \supset ((P \supset Q) \supset Q)) \supset P)$
$(((\sim\sim Q \supset Q) \supset P) \supset ((\sim\sim Q \supset P) \supset P)) \supset ((\sim\sim P \supset ((P \supset Q) \supset Q)) \supset ((\sim P \supset \sim Q) \supset P))$
$(((\sim\sim Q \supset Q) \supset P) \supset ((\sim\sim Q \supset P) \supset P)) \supset ((\sim\sim P \supset (\sim Q \supset P)) \supset ((\sim\sim P \supset (Q \supset P)) \supset P))$
$(((\sim\sim P \supset P) \supset ((\sim P \supset Q) \supset Q)) \supset ((\sim\sim P \supset Q) \supset (\sim\sim Q \supset Q))) \supset ((\sim\sim Q \supset (P \supset Q)) \supset Q)$

$(((\sim\sim P \supset P) \supset ((\sim P \supset Q) \supset Q)) \supset ((\sim\sim P \supset Q) \supset (\sim\sim Q \supset Q))) \supset ((\sim\sim P \supset ((Q \supset P) \supset P)) \supset Q)$
$(((\sim\sim P \supset P) \supset ((\sim P \supset Q) \supset Q)) \supset ((\sim\sim P \supset Q) \supset (\sim\sim Q \supset Q))) \supset ((\sim\sim P \supset ((Q \supset P) \supset P)) \supset ((P \supset Q) \supset Q))$
$(((\sim\sim P \supset P) \supset ((\sim P \supset Q) \supset Q)) \supset ((\sim\sim P \supset Q) \supset (\sim\sim Q \supset Q))) \supset ((\sim\sim P \supset ((Q \supset P) \supset P)) \supset ((\sim Q \supset \sim P) \supset Q))$
$(((\sim\sim P \supset P) \supset ((\sim P \supset Q) \supset Q)) \supset ((\sim\sim P \supset Q) \supset (\sim\sim Q \supset Q))) \supset ((\sim\sim Q \supset ((Q \supset P) \supset Q)) \supset Q)$
$(((\sim\sim Q \supset Q) \supset ((\sim Q \supset P) \supset P)) \supset ((\sim\sim Q \supset P) \supset (\sim\sim P \supset P))) \supset ((\sim\sim P \supset ((P \supset Q) \supset P)) \supset P)$
$(((\sim\sim Q \supset Q) \supset ((\sim Q \supset P) \supset P)) \supset ((\sim\sim Q \supset P) \supset (\sim\sim P \supset P))) \supset ((\sim\sim P \supset ((P \supset Q) \supset P)) \supset ((Q \supset P) \supset P))$
$(((\sim\sim Q \supset Q) \supset ((\sim Q \supset P) \supset P)) \supset ((\sim\sim Q \supset P) \supset (\sim\sim P \supset P))) \supset ((\sim\sim P \supset ((P \supset Q) \supset Q)) \supset P)$
$(((\sim\sim Q \supset Q) \supset ((\sim Q \supset P) \supset P)) \supset ((\sim\sim Q \supset P) \supset (\sim\sim P \supset P))) \supset ((\sim\sim P \supset ((P \supset Q) \supset Q)) \supset ((\sim P \supset \sim Q) \supset P))$